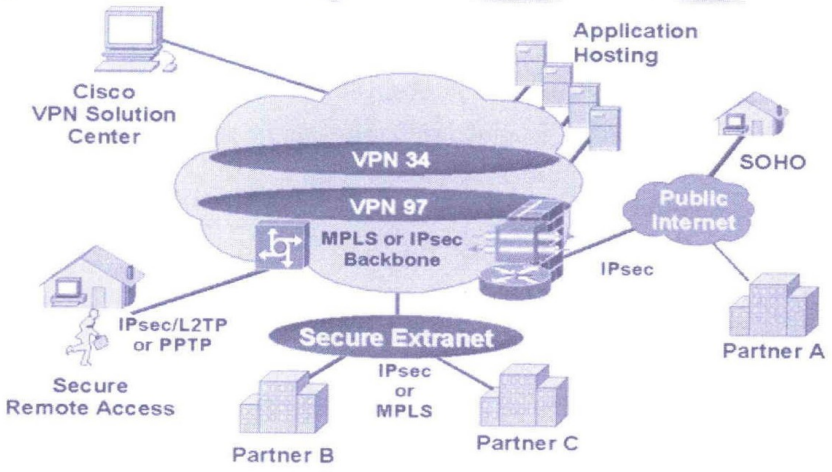
■ ดร.วิรินทร์ เผ่าประดิษฐสิน

Feature

คม-ชัด-ลึก กับระบบเครือข่าย VPN

ไขปริศนาการสร้างเครือข่ายล่องหน VPN
ปฏิบัติการสับสุดยอดเพื่อปกป้องข้อมูลสำคัญ
ให้รอดพ้นจากเงื้อมมือของผู้ก่อการร้าย
ที่แอบแฝงตัวอยู่บนเครือข่ายสาธารณะ



ลักษณะของเครือข่ายทั้งแบบส่วนตัวและแบบสาธารณะสามารถแบ่งแยกได้อย่างชัดเจน เครือข่ายสาธารณะได้แก่เครือข่ายโทรศัพท์สาธารณะและอินเทอร์เน็ตเป็นเครือข่ายที่รวมคอมพิวเตอร์และเครือข่ายระบบต่าง ๆ เข้าด้วยกัน แลกเปลี่ยนข้อมูลข่าวสารระหว่างกันอย่างอิสระ โดยผู้ที่สื่อสารข้อมูลบนอินเทอร์เน็ตไม่จำเป็นต้องมีระบบเครือข่ายรวมทั้งอุปกรณ์คอมพิวเตอร์ที่เหมือนกัน เพียงแต่ต้องทำงานภายใต้โปรโตคอลการสื่อสารเดียวกัน

เครือข่ายส่วนตัวประกอบด้วยคอมพิวเตอร์ที่เชื่อมโยงกันภายในองค์กรและแบ่งปันทรัพยากรร่วมกัน โดยมีหลักประกันที่แน่นอนว่าเฉพาะบุคคลในองค์กรเท่านั้นที่สามารถสื่อสารและใช้ทรัพยากรที่มีอยู่ บุคคลภายนอกเครือข่ายไม่สามารถเข้ามาร่วมใช้งานบนเครือข่ายขององค์กรได้ถึงแม้ว่าจะมีการเชื่อมโยงกันระหว่างสาขาขององค์กรก็ตาม อุปกรณ์การสื่อสารหรือช่องทางการสื่อสารก็ดีขณะที่ยังมีการเชื่อมโยงในลักษณะเครือข่าย บุคคลที่มาจากเครือข่ายอื่นไม่สามารถเข้าร่วมใช้เครือข่ายนี้ได้เช่นเดียวกัน

การเชื่อมต่อระหว่างเครือข่ายขององค์กรเดียวกันในระยะทางไกลนั้นสามารถทำได้โดยการเช่าคู่สายโทรศัพท์ของผู้ให้บริการ เช่น องค์การโทรศัพท์ฯ ซึ่งอาจต้องเสียค่าใช้จ่ายที่คิดเป็นนาทีหรือแบบรายเดือนหากเป็นการเชื่อมต่อภายในประเทศ แต่ถ้าเป็นการเชื่อมต่อระหว่างประเทศจะต้องเสียค่าโทรศัพท์ทางไกลระหว่างประเทศที่คิดเป็นนาทีเช่นกัน

การเชื่อมต่อเครือข่ายสำหรับองค์กรที่อยู่ห่างกันระดับจังหวัดหรือระดับประเทศนั้นต้องเสียค่าใช้จ่ายมาก เหตุนี้เครือข่ายอินเทอร์เน็ตซึ่งเป็นเครือข่ายสาธารณะจึงถูกนำมาใช้เพื่อการเชื่อมต่อกันระหว่างองค์กรแบบเครือข่ายส่วนตัว (Private Network) ที่เรียกว่าอินทราเน็ต (Intranet)

เครือข่ายอินทราเน็ตเป็นระบบเครือข่ายที่ใช้ทรัพยากรที่มีอยู่บนอินเทอร์เน็ตเพื่อการสื่อสารข้อมูลระหว่างองค์กรในรูปแบบของเครือข่ายส่วนตัว โดยองค์กรนั้นจะต้องทำงานบนเครือข่าย TCP/IP จากนั้นนำข้อมูลไปวางไว้ที่เว็บไซท์ภายในขององค์กร แล้วใช้เว็บเบราเซอร์อย่างเช่น Netscape และ Internet Explorer เป็นเครื่องมือในการดึงข้อมูลขององค์กรนั้นออกมา

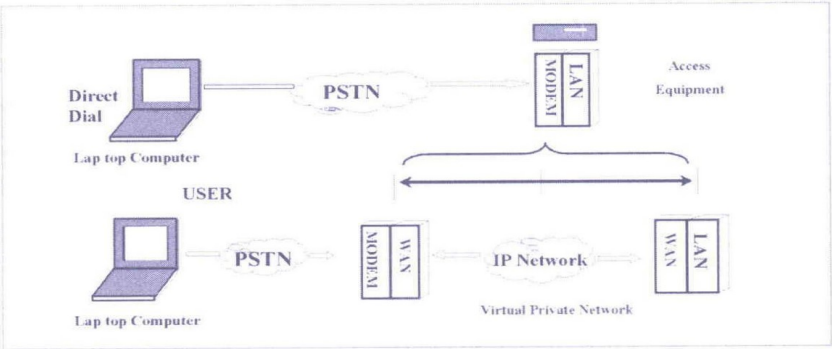
ตัวอย่างการใช้งานอินทราเน็ตได้แก่ ฐานข้อมูลลูกค้าและข่าวสารขององค์กรที่สามารถเข้าถึงได้ทางอินเทอร์เน็ต เจ้าหน้าที่ขององค์กร เช่น ฝ่ายขายสามารถใช้ประโยชน์จากฐานข้อมูลนี้ติดต่อกับลูกค้า เพื่อเสนอขายผลิตภัณฑ์ใหม่ ๆ และเสนอราคาไปในตัว

ด้วยเครือข่ายอินทราเน็ตทำให้ท่านสามารถติดต่อสื่อสารกับองค์กรได้อย่างง่ายดาย และประหยัดค่าใช้จ่ายได้อย่างมาก ทำให้องค์กรทั่วไปนิยมนำระบบอินทราเน็ตไปปฏิบัติอย่างต่อเนื่องเป็นแรมปี แต่แน่นอนเมื่อมีข้อดีก็ต้องมีข้อเสียบ้าง นั่นคือระบบรักษาความปลอดภัยของข้อมูล

เป็นที่ทราบดีว่าเครือข่ายอินเทอร์เน็ตเป็นเครือข่ายสาธารณะ ทุกคนสามารถใช้งานร่วมกัน จึงมักประสบปัญหาเกี่ยวกับความปลอดภัยของข้อมูลข่าวสารที่วิ่งไปมาบนเครือข่ายที่เต็มไปด้วยแฮคเกอร์ ซึ่งคอยจ้องจะล้วงความลับของท่าน แนวทางการป้องกันในเรื่องนี้ไม่ได้อยู่ที่การวางระบบรักษาความปลอดภัยของข้อมูลเพียงอย่างเดียว แต่หัวใจหลักที่ได้ผลดีอย่างแท้จริงได้แก่การสร้างสถาปัตยกรรมการเชื่อมต่อที่ทำให้ผู้ที่อยู่บนอินเทอร์เน็ตหรืออินทราเน็ตไม่มีใครทราบเลยว่าขณะนี้มีการสื่อสารเชื่อมต่อเกิดขึ้นระหว่างองค์กรบนอินเทอร์เน็ต ลักษณะนี้เหมือนกับท่านกำลังคุยกับเพื่อนของท่านกลางตลาดนัดสวนจตุจักร โดยที่คนอื่น ๆ ที่เดินผ่านไปมามองไม่เห็นท่านและเพื่อนของท่าน ระบบที่สามารถทำลักษณะเช่นนี้ได้คือการสร้างเครือข่าย VPN หรือ Virtual Private Network

ลักษณะการทำงานของ VPN

Virtual Private Network เป็นระบบเครือข่ายส่วนตัวขององค์กรที่ทำงานบนเครือข่ายสาธารณะ ตัวอย่างเช่น อินเทอร์เน็ต เหตุผลที่เรียกว่า "Virtual" หรือ "เสมือน" นั้นหมายถึงการเชื่อมต่อและสื่อสารในรูปแบบเสมือนจริง แต่ในทางกายภาพนั้นไม่มีการเชื่อมต่อจริงในทางวงจรเกิดขึ้นเลย แต่มีการส่งข้อมูลในรูปแบบแพ็กเก็ตออกมาที่เครือข่ายอินเทอร์เน็ต ผ่านช่องทางพิเศษที่เรียกว่าอุโมงค์ (Tunnel) ซึ่งอุโมงค์นี้จะถูกสร้างขึ้นระหว่างผู้ให้บริการ VPN กับผู้ใช้บริการ VPN ข้อมูลที่วิ่งเข้าสู่อุโมงค์นี้จะถูกเข้ารหัส (Encrypted) และนำไปถอดรหัสที่ปลายทาง ปกติอุโมงค์นี้ไม่สามารถถูกดักจับได้อยู่แล้ว เนื่องจากถูกสร้างขึ้นบนพื้นฐานของการที่ไม่ได้ล็อคคู่สายระหว่างผู้รับกับผู้ส่งทางกายภาพ ดังนั้นเมื่อมีการเข้ารหัสประกอบกับกรรมวิธีการพิสูจน์สิทธ์การใช้งานเข้าไปอีกชั้นหนึ่ง ยิ่งทำให้เครือข่าย VPN มีความเหมาะสมสำหรับใช้เป็นเครือข่ายส่วนตัวบนอินเทอร์เน็ตที่มีความปลอดภัย



รูปที่ 1 เปรียบเทียบลักษณะการเชื่อมต่อระหว่างเครือข่ายแบบเก่ากับ VPN

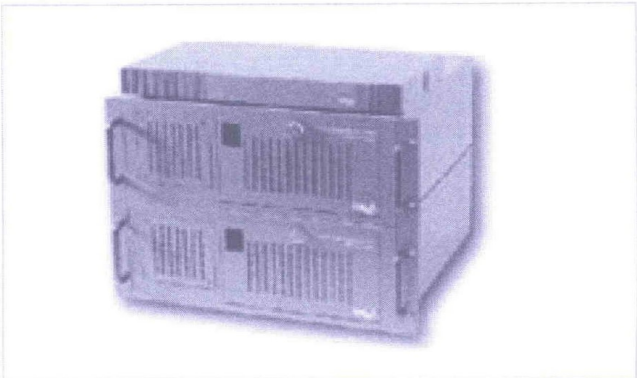
เครือข่าย VPN ทำให้ผู้ใช้คอมพิวเตอร์ภายในองค์กรสามารถทำงานที่บ้านหรือภายนอกบริษัทด้วยการสื่อสารข้อมูลกับเครือข่ายของบริษัทได้อย่างปลอดภัย โดยการใช้โครงข่ายที่มีอยู่ (เช่น อินเทอร์เน็ต) ในมุมมองของผู้ใช้จะเห็นว่า VPN เป็นเครือข่ายที่มีการเชื่อมต่อระหว่างจุด (Point To Point) ระหว่างคอมพิวเตอร์ของผู้ใช้กับเซิร์ฟเวอร์ขององค์กร นอกจากนี้ VPN ยังให้บริการการสื่อสารข้อมูลที่มีความปลอดภัยสูงระหว่างองค์กรกับองค์กรด้วยกันบนอินเทอร์เน็ตได้อีกด้วย

ชนิดของ VPN ที่มีอยู่ในปัจจุบัน

ชนิดของ VPN ที่ใช้อยู่ในปัจจุบันมีถึง 4 แบบ ครั้นจะบอกว่าแบบไหนดีที่สุดย่อมขึ้นอยู่กับแอพพลิเคชันที่ใช้ งบประมาณที่มีรวมทั้งความช่ำชองทางเทคนิคของท่าน

- **Hardware Based VPN** : ผลิตภัณฑ์นี้โดยทั่วไปจะเป็นอุปกรณ์ประเภท Standalone พร้อมโปรเซสเซอร์ที่ใช้ประมวลผลสำหรับงาน VPN โดยเฉพาะ เช่น ทำหน้าที่ดูแลเกี่ยวกับการขอสิทธิ์และให้สิทธิ์การใช้งาน รวมทั้งการหุ้มห่อแพ็กเก็ต การเข้ารหัสและการคัดสรรผู้มีสิทธิ์เข้ามาใช้เครือข่าย ผลิตภัณฑ์นี้ให้ประสิทธิภาพในการทำงานที่ดีกว่า เนื่องจากเน้นการออกแบบเพื่อการนี้โดยเฉพาะ อุปกรณ์ในตัวอย่างนี้ได้แก่ Virtual Access Server หรือ Router ที่สนับสนุน VPN เป็นต้น

รูปที่ 2 แสดงอุปกรณ์ที่สนับสนุน VPN



● **Software Based VPN** : ปัจจุบันมีผลิตภัณฑ์เซิร์ฟเวอร์หลายรายการที่ต่างระบุว่าสนับสนุน VPN รวมทั้งสนับสนุน Remote Access หรือ Routing Module ซึ่งผลิตภัณฑ์เหล่านี้ให้บริการสนับสนุนเพียงขั้นพื้นฐานเท่านั้น รวมทั้งจะมีข้อจำกัดมากพอสมควร เนื่องจากโปรเซสเซอร์ที่ติดตั้งไว้ในสินค้านี้จะต้องทำงานหลายด้าน แทนที่จะทำงานกับ VPN อย่างเดียวเท่านั้น

● **Firewall-Based VPN** : ถือได้ว่าเป็น Software Based VPN อย่างหนึ่ง แต่แตกต่างกันตรงที่ซอฟต์แวร์นี้มีการเพิ่มไฟร์วอลล์เข้าไป ซึ่งผลิตภัณฑ์ซอฟต์แวร์ประเภทไฟร์วอลล์ส่วนใหญ่จะเพิ่ม IPSec (มาตรฐานโปรโตคอลของ VPN) เพื่อสนับสนุนผลิตภัณฑ์นี้

● **การให้บริการ VPN จาก ISP** : ปัจจุบันมี ISP หลายรายที่ให้บริการบริหารจัดการระบบ VPN โดยการใช้ผลิตภัณฑ์ Hardware Based หรือ Firewall Based VPN ซึ่งทาง ISP เป็นผู้ลงทุนดำเนินงานเอง ข้อพิจารณาที่ท่านพึงระวังก็คือระบบโครงข่ายรักษาความปลอดภัยของท่านมิได้อยู่ในมือของท่าน ซึ่งท่านจะต้องมอบความไว้วางใจแก่ ISP รายนั้น

ส่วนประกอบที่เป็นกุญแจสำคัญของ VPN

ส่วนประกอบสำคัญซึ่งขาดไม่ได้สำหรับ VPN ได้แก่

● **Authentication VPN** จะต้องสามารถตรวจสอบและพิสูจน์ความมีสิทธิ์ในการเข้าถึงเพื่อใช้งานเครือข่าย เป็นการยืนยันว่าผู้นั้นมีสิทธิ์ใช้งานจริง โดยยึดกลไกการพิสูจน์สิทธิ์หลายประการ หลังจากที่ผ่านการพิสูจน์สิทธิ์แล้ว VPN จึงจะสร้างอุโมงค์ของการเชื่อมต่อขึ้นเพื่อเชื่อมโยงระหว่างเซิร์ฟเวอร์หรือเครือข่ายองค์กรกับผู้ใช้งานที่มีสิทธิ์นั้นในทันที

● **Encapsulation** เมื่ออุโมงค์ถูกเปิดข้อมูลข่าวสารที่จะวิ่งไปมาภายในอุโมงค์จะต้องได้รับการห่อหุ้มโดย IP Packet ที่ทำงานภายใต้โปรโตคอลของ VPN การใช้ Encapsulation หรือการห่อหุ้มแพ็กเก็ตของข้อมูลข่าวสารเช่นนี้จะช่วยให้ข้อมูลข่าวสารที่ทำงานบนโปรโตคอลของเครือข่ายที่ไม่ใช่ IP เช่น IPX หรือ Apple Talk สามารถวิ่งผ่านเครือข่ายที่ใช้ IP ดังเช่นอินเทอร์เน็ตได้ นอกจากนี้ VPN Server หรือ VPN Software ที่ทำงานบนมาตรฐานของ IPSec จะทำการห่อหุ้มแพ็กเก็ตของ IP อีกชั้นหนึ่ง เพื่อการตรวจสอบแพ็กเก็ตชนิดที่เรียกว่าตัวต่อตัว ทำให้แพ็กเก็ตของข้อมูลที่ปลอมปนมาไม่สามารถเล็ดลอดเข้ามาในอุโมงค์ได้อย่างเด็ดขาด และ IPSec ซึ่งเป็นหนึ่งในโปรโตคอลการทำงานของ VPN นี้ยังสามารถทำงานร่วมกับ Network Firewall โดยทั่วไปได้อีกด้วย

● **Encryption** ในการส่งข้อมูลออกจากเครือข่ายตัวแพ็กเก็ตต้องผ่านการเข้ารหัสเสียก่อน เพื่อป้องกันนักโจรกรรมข้อมูลที่ใช้วิธีการที่เรียกว่า Sniffer ด้วยวิธีการเข้ารหัสหลากชนิด ซึ่งผลิตภัณฑ์ VPN โดยทั่วไปจะให้บริการวิธีการเข้ารหัสได้หลายชนิด ทำให้ผู้ดูแลเครือข่ายสามารถเลือกว่าจะใช้เพื่อป้องกันข้อมูลในระดับใดได้บ้าง

● **Policy-Based Filtering** ผลิตภัณฑ์ VPN โดยทั่วไปจะมีการทำงานคล้ายกับไฟร์วอลล์ กล่าวคือ สามารถกำหนดได้ว่าจะให้ผู้มีสิทธิ์ Access เข้ามาที่เครือข่ายในระดับใดได้บ้าง โดยการกำหนดให้แต่ละคนมีสิทธิ์พิเศษเป็นราย ๆ ไป

หมายเหตุ : คำว่าอุโมงค์ในที่นี้หมายถึงช่องทางการเชื่อมต่อทางตรรก (ไม่ใช่ทางกายภาพ และไม่ได้หมายถึงสายสัญญาณเชื่อมต่อเฉพาะงาน) ซึ่งผู้มีสิทธิ์เท่านั้นที่สามารถเข้ามาใช้เครือข่ายได้ โดยข้อมูลที่วิ่งไปมาระหว่างผู้ใช้กับเครือข่ายองค์กรจะได้รับการห่อหุ้มให้สามารถวิ่งบนเครือข่าย IP เช่น อินเทอร์เน็ตได้ อีกทั้งข้อมูลข่าวสารที่สื่อสารกันไปมาระหว่างกันยังได้รับการเข้ารหัส ยิ่งกว่านั้นยังมีการตรวจสอบสิทธิ์ของผู้ใช้ก่อนจะเปิดการเชื่อมต่อให้ รวมทั้งจะมีการตรวจสอบความถูกต้องของแพ็กเก็ตที่วิ่งไปมาบนเครือข่ายเพื่อให้แน่ใจว่าถูกต้องจริง จะเห็นได้ว่าการกระทำเช่นนี้เป็นเครือข่ายส่วนตัวที่เกิดขึ้นบนเครือข่ายสาธารณะ จึงคล้ายกับว่าท่านมีช่องทางเดินพิเศษบนท้องถนนที่ไม่มีใครมองเห็นนั่นเอง นี่คือบทสรุปประโยชน์ของ VPN

รูปแบบของ VPN

ปัจจุบันมี VPN อยู่ 3 รูปแบบ ได้แก่

1. ACCESS VPN - ให้บริการ Remote User เช่น Mobile User, Telecommuter และ Branch offices ที่ต้องการ Access เข้าไปที่เครือข่ายขององค์กร

2. INTRANET VPN - อนุญาตให้เครือข่ายสาขาขององค์กรสามารถเชื่อมต่อกับเครือข่ายองค์กรอย่างมั่นคงและปลอดภัย

3. EXTRANET VPN - อนุญาตให้ลูกค้า Supplier และผู้ร่วมค้าสามารถ Access เข้าไปที่เครือข่ายอินทราเน็ตขององค์กรอย่างมั่นคงและปลอดภัย

ส่วนประกอบของ VPN

VPN มีส่วนประกอบดังนี้

- VPN Client
- Network Acess Server (NAS)
- อุปกรณ์ Tunnel Terminating Device (หรือ VPN Server)
- VPN Protocol

VPN CLIENT

หมายถึงเครื่องคอมพิวเตอร์ของผู้ใช้งาน VPN ที่จะต้องได้รับการติดตั้งโปรโตคอลที่สนับสนุน VPN หรืออาจต้องติดตั้งซอฟต์แวร์ที่เกี่ยวกับระบบรักษาความปลอดภัยที่จำเป็น

NAS (Network Access Server)

เป็นอุปกรณ์ที่ใช้สื่อสารผ่านโมเด็มที่ใช้ Analog Telephone หรือวงจร ISDN ซึ่งอุปกรณ์ต่าง ๆ ของ NAS จะติดตั้งไว้ที่ ISP ซึ่งให้บริการ VPN

VPN Server

VPN Server อาจอยู่ใน POP ของ ISP หรือที่ตั้งขององค์กรหลัก (ขึ้นอยู่กับโมเดลของ VPN)

VPN Protocol

มี Protocol ที่เป็น Tunnelling Protocol 4 แบบ และมีอยู่ 3 แบบเป็น Extension ของ PPP ได้แก่

- Point-To-Point Tunnelling Protocol (PPTP)
- Layer 2 Forwarding (L2F)
- Layer 2 Tunnelling Protocol (L2TP)
- IP Security (IPSEC) Protocol Suite

โปรโตคอลทั้ง 4 นี้สามารถแบ่งเป็น 2 กลุ่มใหญ่ ๆ ได้แก่

- Layer 2 Tunnelling Protocol
- Layer 3 Tunnelling Protocol

* PPTP, L2F และ L2 TP = Layer 2 Tunnelling Protocol
* IPSec = Layer 3 Tunnelling Protocol

โปรโตคอลที่ทำงานบน Layer 2

Layer 2 Tunnelling Protocol ทำงานบน Data link layer ซึ่งเป็นเลเยอร์ที่ 2 บนโมเดล OSI มีหน้าที่นำแพ็กเก็ตใน Layer 3 มาหุ้มห่อด้วยโปรโตคอลในระดับ Layer 2 ได้แก่ PPP ก่อนที่จะหุ้มห่อด้วย IP Packet อีกชั้นหนึ่ง เมื่อเป็นเช่นนี้กระบวนการรักษาความปลอดภัยจะใช้ของ PPP ซึ่งมีวิธีการพิสูจน์สิทธิ์การใช้งาน ซึ่งได้แก่ PAP และ CHAP (ดังรูปที่ 3)

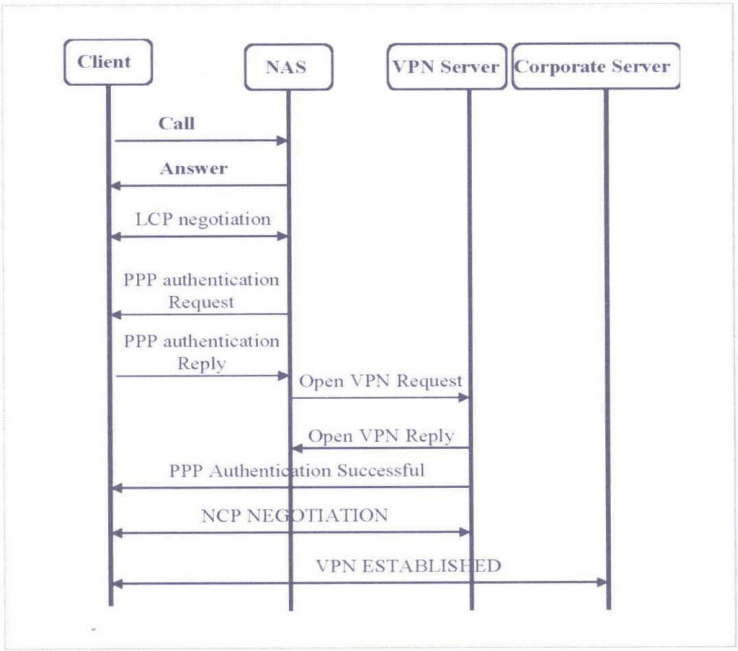
1. Client หรือผู้ใช้งานที่เรียกเข้ามาที่ NAS (Network Access Server) โดยทางโทรศัพท์ด้วยโปรโตคอล PPP โดยตัว NAS เป็นอุปกรณ์ทางฮาร์ดแวร์ประกอบด้วย Remote Access Server หรือ Remote Access Switch ซึ่งติดตั้งอยู่ที่ ISP หรือผู้ให้บริการเครือข่าย

2. การเรียกเข้ามาของ Client จะได้รับการตอบรับจากผู้ให้บริการ

3. ทั้ง Client และ NAS จะใช้ LCP Frame ซึ่งเป็นเฟรมที่ใช้สื่อสารภายใต้ PPP เพื่อติดต่อกัน

4. NAS จะใช้โปรโตคอลพิสูจน์สิทธิ์ ซึ่งได้แก่ PAP หรือ CHAP

5. หลังจากที่ผ่านการพิสูจน์สิทธิ์เรียบร้อยแล้ว NAS จะขอติดต่อกับ VPN Server เพื่อขอให้เปิดช่องใช้งานบน VPN ซึ่ง VPN Server จะตอบรับกลับมาโดยดี



รูปที่ 3 แสดงให้เห็นขั้นตอนการเชื่อมต่อเพื่อสร้างอุโมงค์ VPN

6. เมื่อถึงขั้นตอนนี้เท่ากับว่าการพิสูจน์สิทธิ์ภายใต้โปรโตคอล PPP เป็นอันเสร็จสิ้นโดยสมบูรณ์

7. คอมพิวเตอร์ของผู้ใช้กับ VPN Server จะใช้โปรโตคอล NCP เพื่อตรวจสอบการเชื่อมต่อในขั้นตอนสุดท้าย รวมทั้งคุณภาพของการเชื่อมต่อ

8. สุดท้ายแล้วอุโมงค์การเชื่อมต่อ VPN จะถูกจัดสร้างขึ้นอย่างสมบูรณ์

รูปแบบโปรโตคอลของ VPN บน Layer 2

โปรโตคอลของ VPN ที่ทำงานบนระดับชั้น Layer 2 ในโมเดล OSI มี 3 แบบดังนี้

L2F (Layer 2 Forwarding protocol)

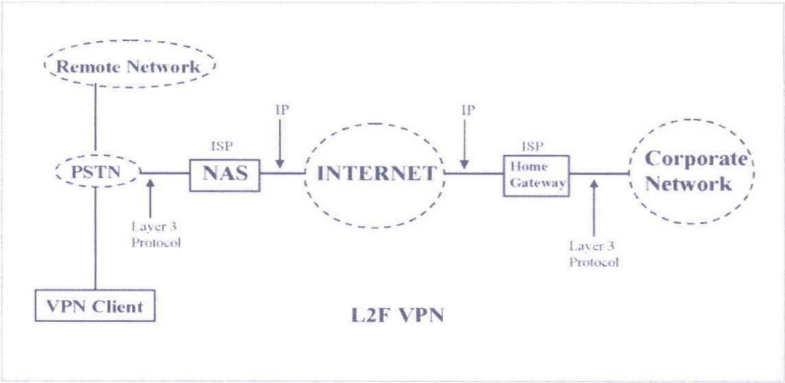
L2F เป็นโปรโตคอลที่พัฒนาโดยบริษัท CISCO System เป็นโปรโตคอลการทำงานอิสระที่สามารถทำงานบนเครือข่าย X.25 เฟรมรีเลย์ และเครือข่าย ATM โปรโตคอลนี้สนับสนุนเครือข่าย IP ส่วนตัว เครือข่ายที่ใช้โปรโตคอล IPX และ Apple Talk และสามารถใช้โปรโตคอล UDP เพื่อการสร้างอุโมงค์ของการเชื่อมต่อบนอินเทอร์เน็ต นอกจากนี้ L2F ยังได้นิยามมาตรฐานการเชื่อมต่อหลากชนิดภายในอุโมงค์ ทำให้อุโมงค์หนึ่งสามารถสนับสนุนคุณลักษณะการเชื่อมต่อได้มากมายหลายแบบ

ภายใต้การใช้งาน L2F ตัว VPN Server นั้นจะเรียกว่า Home Gateway และ L2F ใช้โปรโตคอล PPP เพื่อการตรวจสอบสิทธิ์การใช้งานตั้งแต่เริ่มโทรศัพท์เข้ามาที่เครือข่าย นอกจากนี้ L2F ยังสนับสนุนรูปแบบของการพิสูจน์สิทธิ์การใช้งานแบบอื่น ๆ เช่น RADIUS และ TACACS+ รูปแบบการเชื่อมต่อจะแสดงในรูปที่ 4

โปรโตคอล L2F ต่างจากโปรโตคอล PPTP ตรงที่ L2F ได้กำหนดมาตรฐานการสร้าง Header ของตัวเองโดยไม่ขึ้นกับ IP และ GRE ความสามารถนี้เองที่ทำให้ L2F สามารถทำงานบนเครือข่ายต่างชนิดกันได้

L2F HEADER	SLIP/PPP PAYLOAD	L2F CHECK SUM (OPTIONAL)

● SLIP/PPP Payload จะถูกห่อหุ้มไว้ ใน L2F Packet ร่วมกับ L2F Header และมี Optional L2F Checksum เป็นส่วนหางของแพ็กเก็ต



รูปที่ 4 แสดงการเชื่อมต่อ VPN ภายใต้โปรโตคอล L2F

โปรโตคอล PPTP

PPTP เป็นโปรโตคอลที่พัฒนาโดย Microsoft และกลุ่มผู้ผลิตอุปกรณ์เครือข่ายชั้นนำหลายแห่ง รวมทั้ง ASCEND Communication และ 3COM โปรโตคอลนี้ยอมให้โปรโตคอลในระดับเครือข่าย เช่น IPX, NETBUEI และ IP ที่สื่อสารข้อมูลในรูปแบบแพ็กเก็ตสามารถถูกหุ้มห่อไว้ภายในแพ็กเก็ตของ IP ได้ จึงทำให้งานแอพพลิเคชันที่ไม่ได้ใช้ IP สามารถวิ่งอยู่บนเครือข่ายอินเทอร์เน็ตได้

เนื่องจากเป็นโปรโตคอล PPTP เป็นส่วนต่อเติมของโปรโตคอล PPP ดังนั้นจึงสนับสนุนเฉพาะการเชื่อมต่อแบบจุดต่อจุด (Point-To-Point) แต่จะไม่สนับสนุนการเชื่อมต่อกับปลายทางที่มีหลาย ๆ จุด (Point-To-Multipoint) และที่สำคัญคือโปรโตคอล PPTP เป็นโปรโตคอลที่เอนเอียงไปทาง IP (IP-Centric Protocol) ที่ออกแบบมาเพื่อให้ทำงานบนเครือข่าย IP เท่านั้น

ในการทำงานของ PPTP อุปกรณ์ที่เรียกว่า NAS (Network Access Server) ซึ่งหากอยู่ภายใต้การทำงานของ PPTP เรียกว่า PAC (PPTP Access Concentrator) จะเป็นอุปกรณ์ที่ยอมให้ผู้ใช้เครือข่ายที่จะเข้ามาทางโทรศัพท์สามารถเริ่มสร้างการเชื่อมต่อ VPN (VPN Call) ได้ ส่วน VPN Server จะเรียกว่า PPTP Network Server (PNS) แทนดังรูปที่ 5

โปรโตคอล PPTP เป็นโปรโตคอลประเภทสร้างอุโมงค์ (Tunnelling Protocol) โดยทำหน้าที่นำข้อมูลในรูปแบบของแพ็กเก็ตที่วิ่งภายใต้โปรโตคอลเครือข่าย (เช่น IP NETBUEI หรือ IPX/SPX) มาสอดใส่และถูกหุ้มไว้ (Encapsulation) ใน Packet IP พิเศษ ซึ่งจะทำให้อุปกรณ์เราเตอร์และเครื่องคอมพิวเตอร์ที่พบเห็นเกิดความเข้าใจผิดคิดว่า นี่เป็น Packet IP ขนานแท้และดั้งเดิม การกระทำเช่นนี้เรียกว่าการทำ IP Tunnelling ซึ่งเป็นประโยชน์ต่อการทำให้โปรโตคอลเครือข่ายหลายตัวที่ไม่ใช่ IP สามารถวิ่งผ่านโครงข่ายประเภท IP ได้ เช่น อินเทอร์เน็ต

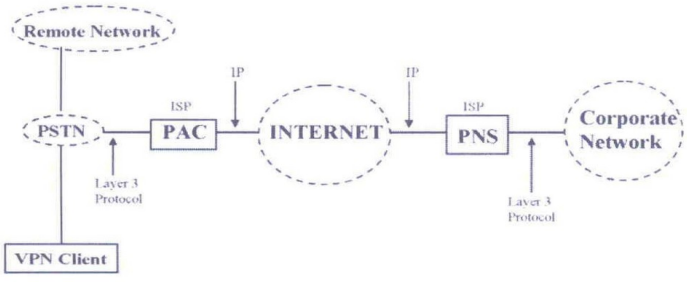
โปรโตคอลออกแบบมาเพื่อให้ผู้ใช้งานสามารถเชื่อมต่อกับ RAS Server จากจุดใด ๆ ก็ได้บนอินเทอร์เน็ต โดยที่ยังต้องมีความเข้มงวดในการเข้าถึงเครือข่ายจากระยะไกล (Remote Access) แทนที่จะใช้โมเด็มเพื่อเชื่อมต่อเข้า RAS Server (Remote Access Server) โดยตรง แต่กลับเชื่อมต่อผ่านทาง ISP แทน โดยจะใช้โปรโตคอล PPTP เพื่อจัดตั้งการ "เรียก" เข้าสู่เซิร์ฟเวอร์ผ่านทางอินเทอร์เน็ต ซึ่งโปรโตคอล PPTP กับ RAS จะใช้วิธีการพิสูจน์แบบมีเอกลักษณ์เฉพาะ รวมทั้งวิธีการเข้ารหัสข้อมูลเพื่อจัดตั้ง VPN

รูปแบบการใช้ VPN ของโปรโตคอล PPTP มี 2 รูปแบบดังนี้

● **แบบที่หนึ่ง : ผู้ใช้งานที่จะเข้าสู่เครือข่ายจากระยะไกลจะต้องหมุนโทรศัพท์เข้ามาที่ ISP ที่ติดตั้ง Remote Access Switch ซึ่งสนับสนุนกรทำงานของ PPTP เป็นการเฉพาะ และ Remote Access Switch เชื่อมต่อกับ RAS Server อีกทีหนึ่ง**

● **แบบที่ 2 : ผู้ใช้งานที่จะเข้าสู่เครือข่ายจากระยะไกลจะหมุนโทรศัพท์เข้ามาที่ ISP ซึ่งไม่สนับสนุนการทำงานของ PPTP แต่จะใช้ PPTP บนเครื่องของผู้ใช้งานเป็นผู้สร้างการเชื่อมต่อ PPTP**

รูปที่ 5 แสดงลักษณะการเชื่อมต่อบนโปรโตคอล PPTP



รูปแบบที่สนับสนุนโปรโตคอล PPTP

รูปแบบการโทรศัพท์เข้ามาที่ ISP ซึ่งสนับสนุน PPTP จะต้องมีปัจจัย 3 ประการดังนี้

- เครือข่ายที่ต้องการจัดตั้งการเชื่อมต่อ VPN จะต้องมี RAS Server ที่ทำงานบน Windows NT 4.0 และตั้งคอนฟิกให้สามารถสนับสนุน PPTP รวมทั้งจัดตั้งช่องสัญญาณสำหรับโทรศัพท์เข้าให้สนับสนุน VPN ส่วนเซิร์ฟเวอร์ต้องสามารถเข้าถึงได้ทางอินเทอร์เน็ต
- ISP ที่โทรศัพท์เข้ามาจะต้องมี Remote Access Switch ที่สนับสนุน PPTP ซึ่งในรูปที่ 5 เรียกว่า PAC ตัวอย่างของอุปกรณ์นี้ได้แก่ Ascend MAX 4004 หรือ U.S. Robotics Total Control Enterprise Network Hub เป็นต้น
- ISP ของท่านจะต้องสามารถให้บริการ PPTP แก่ผู้ใช้งาน รวมทั้งมีรายชื่อสมาชิกที่มีสิทธิ์อยู่ที่ ISP ด้วยเช่นกัน

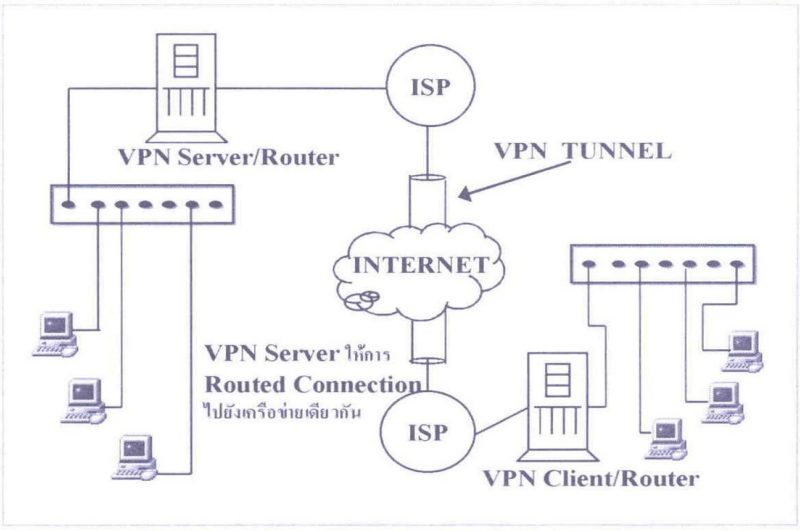
รูปแบบที่ไม่สนับสนุน PPTP

รูปแบบการเชื่อมต่อแบบนี้จะต้องมีปัจจัย 2 ประการ กล่าวคือ ท่านจะต้องติดตั้ง Windows NT RAS Server พร้อมด้วย PPTP บนเครือข่ายของท่าน ซึ่ง RAS Server จะต้องสามารถเข้าถึงทางอินเทอร์เน็ตได้ ประการที่สองเครื่องของผู้ใช้ที่ทำงานบน Windows 95 หรือ NT ต้องติดตั้งโปรโตคอล PPTP และ Dial-UP Networking รูปแบบการเชื่อมต่อจะเป็นดังรูปที่ 6

อย่างไรก็ตามโปรโตคอล PPTP มิได้มีหน้าที่ในการเข้ารหัสข้อมูลที่แพ็กเก็ตของข้อมูลแต่ละตัว แต่อาศัยวิธีการพิสูจน์สิทธิ์การใช้งานที่มีชื่อว่า PAP (Password Authentication Protocol - โปรโตคอลที่ให้บริการพิสูจน์สิทธิ์ด้วยรหัสผ่านแบบ 2 ทาง) และ CHAP (Challenge Handshake Authentication Protocol - โปรโตคอลที่ใช้ Hash Function ทำให้รหัสผ่านที่ป้อนจะถูกเข้ารหัสแบบทางเดียวเข้าสู่เซิร์ฟเวอร์ ทำให้รหัสผ่านไม่สามารถถูกแกะได้โดยง่าย) อีกทั้งตัวแพ็กเก็ตที่เป็น PPTP จะถูกสวมด้วย Header ชื่อ Generic Routing Encapsulation (GRE) อีกทีหนึ่งก่อนที่จะส่งออกไปที่เครือข่าย IP

รูปที่ 7 เป็นหน้าตาของแพ็กเก็ตสำหรับโปรโตคอล PPTP ดังรูปที่ 7

เทคนิคการสวมหรือหุ้มแพ็กเก็ตทำได้โดยใช้มาตรฐานเฉพาะที่ชื่อว่า GRE เพื่อนำมาสร้างอุโมงค์การสื่อสารบนอินเทอร์เน็ต (ปัจจุบันนิยมใช้มาตรฐาน GREv2 ซึ่งเป็นส่วนต่อเติมของ PPTP ให้สามารถกำหนดเลขหมายประจำตัวผู้เรียก รวมทั้งความเร็วในการเชื่อมต่อ



รูปที่ 6 แสดงการเชื่อมต่อ VPN ผ่านบริการของ ISP

รูปที่ 7 แสดงรูปแบบของ PPTP Header ที่ทำงานบนอินเทอร์เน็ต

จากรูปที่ 7 จะเห็นว่า IP Header ประกอบด้วยข้อมูลข่าวสารที่จำเป็นสำหรับ Packet IP เช่น แสดงขนาดของแพ็กเก็ตและที่อยู่ของผู้รับหรือผู้ส่ง ส่วน GRE Header (หรือ GREv2) ประกอบด้วยข้อมูลข่าวสารเกี่ยวกับชนิดของแพ็กเก็ตที่ถูกห่อหุ้มอยู่ภายใน เช่น ข้อมูลข่าวสาร PPTP ที่เกี่ยวข้องกับการสื่อสารระหว่างผู้ใช้งานกับเซิร์ฟเวอร์ ส่วน PPP Header เป็นส่วนของข้อมูลข่าวสารที่โปรโตคอลใช้ทำงานตามปกติ

PPTP เป็นโปรโตคอลที่เหมาะสม ซึ่ง VPN ส่วนใหญ่จะทำงานบนพื้นฐานของโปรโตคอลชนิดนี้ PPTP โปรโตคอล TCP ในการขนถ่ายข้อมูล ดังนั้นจึงสนับสนุนการควบคุมการไหลเวียนของข้อมูลข่าวสาร รวมทั้งการควบคุมอัตราการขนส่งข้อมูลที่จะส่งทำให้ไม่ต้องประสบปัญหาเรื่อง Retransmission อันเนื่องมาจากการโยนแพ็กเก็ตทิ้งเมื่อเกิดปัญหาแพ็กเก็ตล้น

PPTP Tunnel ทำจากอะไร

PPTP ทำให้เกิดการสร้างอุโมงค์เชื่อมต่อสื่อสารโดยการเข้ารหัสข้อมูลข่าวสาร จากนั้นจะทำการหุ้มห่อแพ็กเก็ตข้อมูลนั้นอีกชั้นหนึ่ง อุโมงค์ของ PPTP นี้จะถูกสร้างขึ้น ณ ส่วนบนของเน็ตเวิร์กอินเทอร์เฟสหรือ LAN Card ที่ IP ใช้อยู่ ดังนั้นผู้ใช้ที่ทำงานบน IP สามารถใช้ซอฟต์แวร์ที่สนับสนุน PPTP เพื่อการสร้างอุโมงค์ดังกล่าวได้ ดังรูปที่ 8

อุโมงค์นี้จะต้องวิ่งบนเครือข่าย IP ไม่ว่าจะวิ่งบน LAN หรือเครือข่ายชนิดใดก็ตาม ขอให้เป็น IP เป็นใช้ได้

อุโมงค์นี้สร้างขึ้นโดย Generic Routing Encapsulation (GRE) ซึ่ง GRE เกิดขึ้นขณะที่มีการทำงานในอุโมงค์ โดยภายในของช่องสัมภาระ (Payload) ภายใน GRE จะเป็น PPP Packet พร้อมด้วยข้อมูลที่ผ่านการเข้ารหัสเรียบร้อยแล้ว ในรูปที่ 9 แสดงขั้นตอนการเข้ารหัสข้อมูล พร้อมกับการหุ้มห่อแพ็กเก็ตตั้งแต่ระดับชั้นแอพพลิเคชันลงมาจนถึง Data Link ในโมเดล OSI

L2TP (Layer 2 Tunnelling Protocol)

L2TP เป็นโปรโตคอลที่ทำงานแบบเดียวกับ PPTP แต่มีข้อดีที่ได้รับการปรับปรุงให้เหนือกว่าข้อจำกัดบางประการของ PPTP เช่น L2TP ไม่จำเป็นจะต้องวิ่งบนเครือข่าย IP อย่างเดียวเหมือนกับ PPTP เพราะสามารถทำงานบนเครือข่าย ATM Frame Relay และ X.25 ได้ โปรโตคอลนี้สามารถตรวจสอบสิทธิ์ของผู้ใช้ที่ปลายด้านหนึ่งของอุโมงค์ และยังสามารถทำงานควบคู่ไปกับ Secure ID Card (ถ้ามี) ที่เครื่องของผู้ใช้กับไฟร์วอลล์ที่ด้านของเซิร์ฟเวอร์

L2TP เป็นมาตรฐานของ Internet Engineering Task Force (IETF) ซึ่งพัฒนาโดย Microsoft, CISCO, Ascend, 3COM รวมทั้งผู้ผลิตอุปกรณ์เครือข่ายรายอื่น ๆ เป็นมาตรฐานที่รวมประสิทธิภาพการทำงาน L2F (ซึ่งเป็นของ CISCO) กับ PPTP (ของ Microsoft) เข้าด้วยกัน

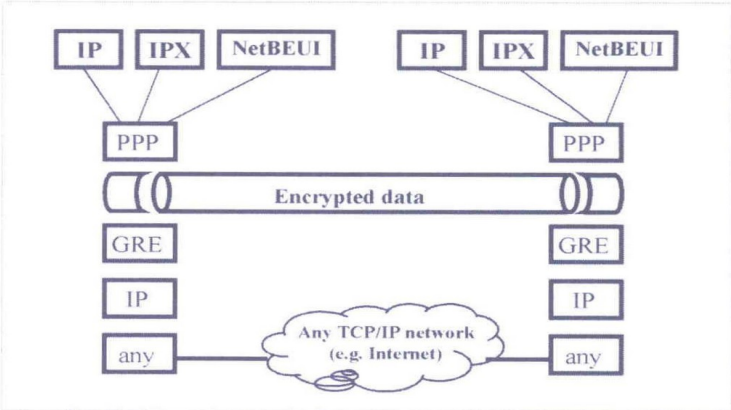
สิ่งที่ L2TP ไม่เหมือนกับ PPTP อีกประการหนึ่งได้แก่ PPTP ทำงานบน TCP ขณะที่ L2TP ทำงานบน UDP ได้อีกทั้งไม่ต้องใช้ GRE เพื่อการหุ้มห่อแพ็กเก็ต เนื่องจากมีซอฟต์แวร์ประเภทไฟร์วอลล์ไม่น้อยที่ไม่สนับสนุน GRE ดังนั้นจึงอาจเกิดปัญหาได้ นอกจากนี้ L2TP เป็นระบบ Firewall VPN แบบหนึ่งที่ใช้งานง่ายกว่า PPTP

ภายใต้โครงข่ายที่ใช้ L2TP อุปกรณ์ NAS จะเรียกว่า L2TP Access Concentrator (LAC) และ VPN Server จะเรียกว่า L2PT Network Server (LNS) ดังรูปที่ 10

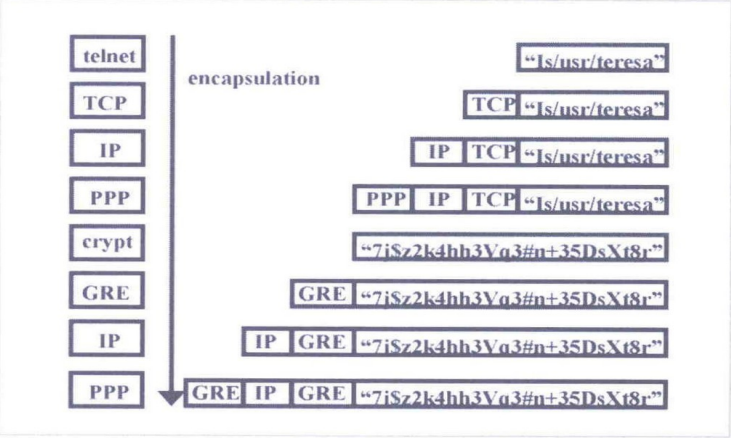
เนื่องจาก L2TP ใช้ PPP โปรโตคอลในการสื่อสารขั้นต้น ดังนั้นจึงยังใช้ PAP และ CHAP เป็นโปรโตคอลในการพิสูจน์สิทธิ์เช่นเคย อย่างไรก็ดี L2TP ยังยอมให้มีการใช้ RADIUS เพื่อการพิสูจน์ตรวจสอบสิทธิ์ของผู้ที่จะเข้ามาใช้งานได้

L2TP อนุญาตให้สร้างหลาย ๆ อุโมงค์เกิดขึ้นในคู่สายแบบตีเกลียว ทำให้ผู้ใช้สามารถสร้างอุโมงค์ที่มีความแตกต่างพร้อมด้วยคุณภาพการให้บริการ (Quality Of Service)

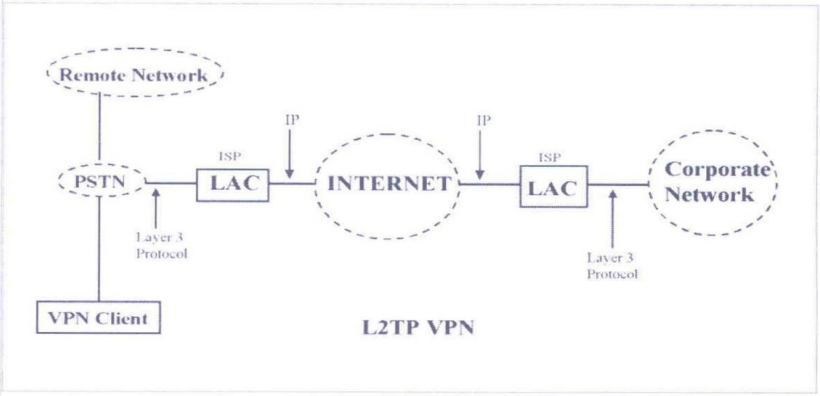
L2TP ขึ้นกับ IPSec ในการเข้ารหัสของข้อมูลข่าวสาร ดังรูปที่ 11



รูปที่ 8 แสดงช่วงของขั้นตอนการเข้ารหัสข้อมูล



รูปที่ 9 แสดงขั้นตอนการเข้ารหัสตั้งแต่ระดับโปรโตคอลสูงสุดลงมาใน OSI model



รูปที่ 10 แสดงการเชื่อมต่อของ VPN ภายใต้ L2TP

ในการเข้ารหัสข้อมูลสามารถทำได้ที่เครื่องคอมพิวเตอร์ของผู้ใช้งาน หรือโดย LAC ทั้งนี้ขึ้นอยู่กับรูปแบบของ VPN ที่นำมาใช้ รูปที่ 12 เป็นขั้นตอนการสื่อสารของ VPN ภายใต้โปรโตคอล L2TP

จากรูปที่ 12 พอจะลำดับขั้นตอนการทำงานได้ดังนี้ (ดูคำอธิบายตามลำดับเลขหมาย)

1. ผู้ใช้ที่เชื่อมต่อเข้ามาทางอินเทอร์เน็ตหรือที่บ้านจะโทรศัพท์มายัง ISP หรือผู้ให้บริการ ผ่านเครือข่ายโทรศัพท์สาธารณะหรือเครือข่าย ISDN ด้วยโปรโตคอลการเชื่อมต่อ PPP

2. หลังจากที่ผู้ให้บริการและผู้ใช้งานทางไกลได้ใช้ PPP เพื่อพิสูจน์สิทธิ์ขั้นพื้นฐานแล้ว การจัดตั้งวงจรเชื่อมต่อขั้นที่หนึ่งก็จะเกิดขึ้น

3. จะมีการส่งชื่อและรหัสผ่านไปที่ ISP Security Server เพื่อตรวจสอบให้แน่ใจอีกครั้ง

4. หลังจากตรวจสอบเรียบร้อยถูกต้องจะมีการสร้างอุโมงค์ การเชื่อมต่อระหว่าง NAS หรือ LAC ที่ติดตั้งอยู่กับ ISP กับ LNS (L2TP Network Server ที่ติดตั้งอยู่ในองค์กรบริษัท)

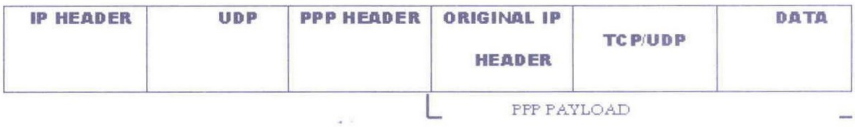
5. หลังจากที่อุโมงค์ถูกเปิดแล้วจะมีการจัดหาช่องส่งสัญญาณสำหรับผู้ใช้ที่ยังไม่มีใครใช้ในขณะนี้ (L2TP สามารถมีหลายคอนเน็กชันในอุโมงค์เดียวกัน) โดยจะมีการส่งข่าวสารที่แสดงถึงการขอเชื่อมต่อออกไปที่ LNS เพื่อให้ LNS รู้ว่ากำลังมีการขอการเชื่อมต่อใหม่เกิดขึ้น เพื่อให้ LAN ยอมรับการเชื่อมต่อในครั้งนี้

6. หาก LNS ตอบรับการขอเชื่อมต่อในครั้งนี้ การสื่อสารระหว่าง LNS และ Server ขององค์กรกับ ISP จะเกิดขึ้น

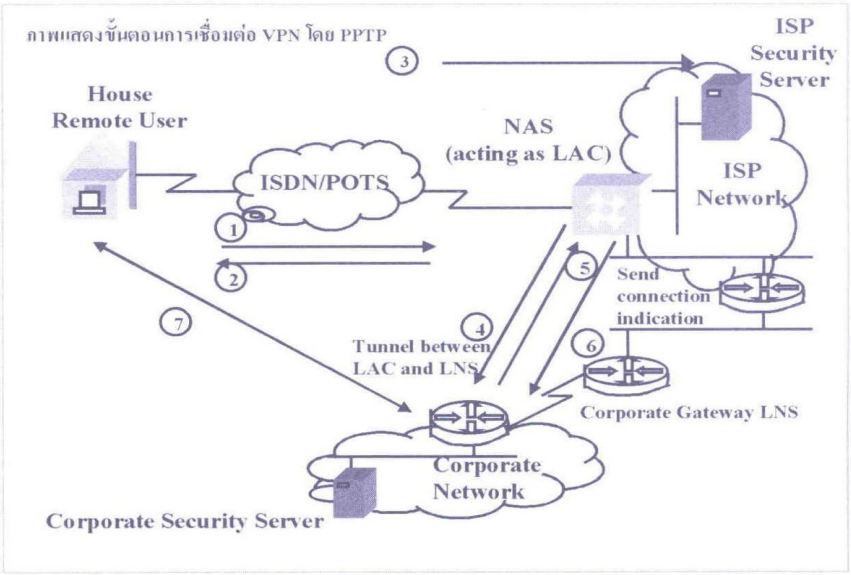
7. และเมื่อนั้นผู้ใช้งานระยะไกลก็สามารถติดต่อกับเซิร์ฟเวอร์ขององค์กรได้โดยผ่านทาง ISP และโยงเข้าที่ LNS มาที่เซิร์ฟเวอร์ขององค์กรได้อย่างปลอดภัย

โปรโตคอล VPN ใน LAYER 3 IPSec

IPSec เป็นระบบรักษาความปลอดภัยที่เพิ่มเติมมาให้กับโปรโตคอล IP ซึ่งจะทำให้เกิดระบบรักษาความปลอดภัยที่มีประสิทธิภาพแก่การสื่อสารบน TCP/IP ซึ่ง IPSec ถูกออกแบบมาให้เป็นระบบรักษาความปลอดภัยที่ทำงานบนพื้นฐานของการเข้ารหัสลับสำหรับ IP Version 4 และ 6 เป็นชุดของกฎกติกาและระเบียบวิธีควบคุมการเข้าถึงเครือข่าย มีการตรวจสอบความถูกต้องของการเชื่อมต่อ ความถูกต้องของที่มาของข้อมูลข่าวสาร ปกป้องการแฝงตัวเข้ามาของบุคคลที่สาม การเข้ารหัส รวมทั้งการควบคุมการไหลเวียนในกระแสของการสื่อสาร ให้การปกป้องโปรโตคอลที่ทำงานในระดับ IP Network Layer) และโปรโตคอลที่สูงกว่านี้



รูปที่ 11 แสดง Packet Format ของ L2TP



รูปที่ 12 แสดงขั้นตอนการทำงานของ VPN ภายใต้ L2TP

IPSec ทำงานอย่างไร

การทำงานของ IPSec จะใช้โปรโตคอลที่ให้บริการควบคุมและรักษาความปลอดภัยขณะที่มีการสื่อสารกันของคู่สนทนาทั้งสองบนเครือข่าย ได้แก่

- IP Authentication Header (AH) ให้บริการตรวจสอบความถูกต้องบนการเชื่อมต่อแบบ Connectionless (การเชื่อมต่อที่ไม่ต้องมีการยืนยันจากคู่สนทนาที่ติดต่อกัน) โดยจะตรวจสอบความถูกต้องของที่มาของข้อมูล รวมทั้งการป้องกันการทำซ้ำของข้อมูลจากบุคคลที่สามได้
- Encapsulating Security Payload (ESP) Protocol ให้บริการการเข้ารหัสลับของข้อมูลข่าวสาร รวมทั้งการจำกัดปริมาณการไหลของการสื่อสาร ทั้งนี้เพื่อป้องกันแฮคเกอร์ที่อาจใช้วิธีการที่เรียกว่า TCP Guessing หรือ TCP SYN Flood เข้ามาโจมตีคู่สนทนาได้

AH กับ ESP ต่างเป็นพาหนะนำไปสู่การควบคุมการเข้าถึงเครือข่ายของผู้ใช้งาน โดยทำงานบนพื้นฐานของการแจกจ่ายหรือการกระจายกุญแจที่ผ่านการเข้ารหัสลับแล้ว รวมทั้งจำกัดปริมาณการไหลของข่าวสารระหว่างคู่สนทนา

สถาปัตยกรรมของ IPSec

ส่วนประกอบหลักของสถาปัตยกรรมนี้ได้แก่

- ระบบบริหารการจัดการกุญแจรหัสลับผ่านทาง Internet Key Exchange (IKE) ซึ่งเดิมเรียกว่า ISAKMP/ Oakley
- ฐานข้อมูลระบบรักษาความปลอดภัยที่ได้กำหนดกฎกติกาการเข้าออกของสัญญาณการสื่อสาร
- โปรโตคอลที่เรียกว่า Authentication Header (AH) ซึ่งจะให้บริการพิสูจน์ความถูกต้องของข้อมูลที่มาจากแหล่งต้นทาง
- ส่วนที่เรียกว่า Encapsulating Security Payload (ESP) ซึ่งจะให้บริการการเข้ารหัส และการตรวจสอบความถูกต้องของข้อมูลข่าวสารจากแหล่งต้นทาง
- IP Packet ที่ใช้เป็นหลักในการส่งข้อมูล

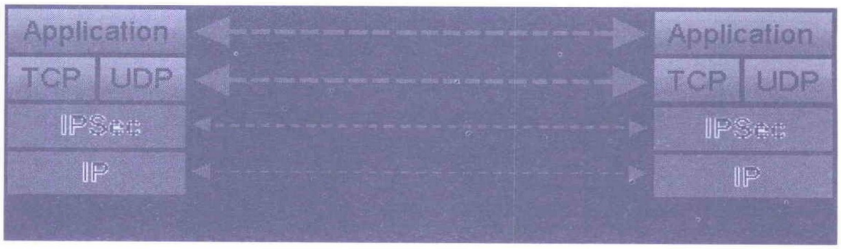
การทำงานของ IPSec มี 2 วิธีคือ ประการแรกได้แก่ Transport Mode ซึ่งเป็นวิธีการที่มีอยู่แล้ว เป็นรูปแบบการถ่ายทอดโดยตรงของข้อมูลที่ได้รับการป้องกันจาก IPSec แล้วจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งดังรูปที่ 13

ประการที่สองได้แก่ Tunnel Mode ด้วยวิธีการนี้ข่าวสารที่สร้างขึ้นมาโดยคอมพิวเตอร์เครื่องหนึ่งที่ไม่ได้สนับสนุน IPSec จะถูกอุปกรณ์รักษาความปลอดภัยหรืออุปกรณ์ Gateway ดักจับ โดยที่ตัวGateway จะทำหน้าที่หุ้มห่อ IP Packet ที่ผ่านการเข้ารหัสโดย IPSec แล้วทั้งหมด (รวมทั้ง IP Header ดั้งเดิม) จากนั้นจะเพิ่ม IP Header ตัวใหม่เข้าไปที่แพ็กเก็ตของข้อมูลนี้ แล้วจึงส่งออกไปยัง Gateway ที่สองของเครือข่ายถัดไป ซึ่งข้อมูลข่าวสารจะถูกถอดรหัสที่ปลายทางดังรูปที่ 14

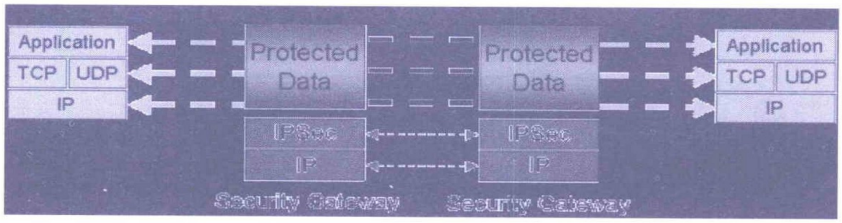
ในกรณีที่ต้องการให้ IPSec วิ่งผ่านตัวไฟร์วอลล์ได้ ท่านจะต้องเปิด UDP Port เลขหมาย 500 (สำหรับ IKE) และ IP Type 50 สำหรับ ESP รวมทั้ง IP Type 51 สำหรับ AH (ปกติ IPSec จะประกอบด้วยส่วนสำคัญสองส่วนได้แก่ ตัว Key Management (IKE Internet Key Exchange)/ISAKMP) ซึ่งใช้บริหารจัดการกุญแจที่เข้ารหัสลับ และส่วนที่เข้ารหัส (ESP))

จุดด้อยของการใช้ IPSec คือการสนับสนุนโดย IP ขณะที่ PPTP L2F และ L2TP สามารถให้การสนับสนุนการสื่อสารข้อมูลที่ไม่ใช่ IP เช่น IPX และ Apple Talk เนื่องจาก PPTP L2F และ L2TP เป็น Layer 2 Protocol

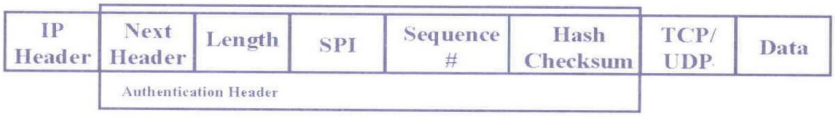
รูปที่ 15 แสดง Packet Header ของ IPSec Protocol



รูปที่ 13 แสดงรูปแบบลักษณะการเชื่อมต่อแบบ Transport Mode



รูปที่ 14 แสดง Tunnel Mode



รูปที่ 15 แสดงลักษณะแพ็กเก็ตของ IPSec

คำอธิบายเกี่ยวกับ Packet ของ AH

- Next Header - หมายถึง Header ตัวต่อไป ในที่นี้ได้แก่ Header ของ TCP หรือ UDP
- Length - เป็นการแสดงขนาดความยาว Header ของ AH
- Security Parameter (SPI) - ใช้เพื่อบ่งบอกว่าแพ็กเก็ตนี้ได้รับการพิสูจน์จากส่วนไหนของ SA
- Sequence Number - เป็นเลขหมายขนาด 32 บิตที่ใช้เพื่อพิสูจน์แสดงลำดับของแพ็กเก็ตตัวนี้ในช่องทางการสื่อสารภายใต้ระบบรักษาความปลอดภัย
- Authentication Data - ใช้เพื่อการตรวจสอบค่าของ Hash (ค่าที่ผ่านการเข้ารหัสเรียบร้อยแล้ว)

ขออำลา

ฉบับหน้าจะเป็นภาคต่อไปของ "คม-ชัด-ลึก กับระบบเครือข่าย VPN" ซึ่งมีเนื้อหาที่เข้มข้นกว่านี้ โดยเน้นหนักในเรื่องของวิธีการเชื่อมต่อในรูปแบบต่าง ๆ รวมทั้งแนะนำอุปกรณ์ทางฮาร์ดแวร์ที่น่าสนใจ และวิธีการติดตั้ง VPN บน Windows NT และ 2000 ตลอดจนระบบปฏิบัติการ LINUX สวัสดีครับ